UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,306	10/14/2005	Yuliang Zheng	56697-326363	1967

44231 7590 08/18/2008

KILPATRICK STOCKTON LLP - 46872
J. STEVEN GARDNER
1001 WEST FOURTH STREET
WINSTON-SALEM, NC 27101

EXAMINER	
HUSSAIN, IMAD	

ART UNIT	PAPER NUMBER
2151	

MAIL DATE	DELIVERY MODE
08/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/553,306	ZHENG ET AL.	
	Examiner	Art Unit	
	IMAD HUSSAIN	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 21 July 2008 has been entered.

2. Claim 1 has been amended. New claim 20 (renumbered to 18) has been added. Claims 1-17 and 20 (renumbered to 18) are pending in application 10/553306.

Response to Arguments

3. Applicant's arguments filed 21 July 2008 have been fully considered, but not found persuasive.

Applicant argues that claim 4 (amended from original filing), directed to a threshold for a service value, would have been an obvious improvement for one of ordinary skill in the art and so should not be rejected under 35 U.S.C. 112.

Examiner has withdrawn the rejection.

Applicant argues that, in regard to claim 1, 13, 18 and their dependent claims, Beavers does not teach *an authorization enforcement facility operable to perform a risk-aware analysis of [a] connection to determine the threat level associated with the connection based at least in part on [a] static policy data attribute*.

In response to the above-mentioned arguments, applicant's interpretation of applied prior art is noted. However, Examiner notes that Beavers does teach an authorization enforcement facility (AEF) [*alert processing system,* claim 12, figure 5 (63)] in communication with the static policy data store [*Rule Engine*, Figure 5 (27)] and the dynamic policy data store [*Decision Tables*, Figure 5 (31)] and operable to perform a risk-aware analysis [*matching* and *declaring an incident*, claim 1] of the connection [via *firewall* of Paragraphs 0002-0003 and connection-monitoring *device experts* of Paragraphs 0104-0114] to determine the threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection based at least in part on the static policy data attribute [*static enterprise data… such as lists of IP addresses that are associated with known attackers,* Paragraph 0077].

Applicant appears to argue that the purpose and role of Beavers' invention and that of the Instant Application differ. Examiner agrees that Beavers focuses on the

portion of the system that receives as input security events generated by devices that monitor security-related threats. However, the disclosure of these monitor devices by Beavers is sufficient in detail to meet the stated limitations of the claimed invention.

Applicant appears to argue that rule matching and security incident declaring is not what is meant by Applicant's use of the phrase "risk analysis." It is unclear to the Examiner how Applicant intends to define said term.

Applicant appears to argue that claimed invention's operability to "store the determined threat level in the dynamic policy data store as a dynamic policy data attribute" is different from Beavers' correlation table storing a set of incident signatures and automatically creating a watch list decision table based on the correlation table.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., lack of user override, internal structure of tables/lists) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant argues that, in regard to claims 6 and 7, Beavers does not teach *blocking the source of the connection from connecting to an intended destination* in response to suspicion of a server being compromised.

In response to Applicant's argument, Examiner notes that shutting down a web server does indeed block the source of the connection from connecting to an intended destination (i.e., the now unavailable web server).

Applicant additionally argues that, specifically in regard to claims 6 and 7, the motivations and methods of Beavers' invention differ from those of Applicant's invention.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., motivation) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Response to Amendment

4. The amendment filed 9 January 2008 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: claim 4 recites a threshold value that is inversely proportional to the **service** value. This limitation is not supported by the specification, wherein it is stated that the threshold value is inversely proportional to the **node** value [Instant Application: Claim 3 and Glossary: Threshold].

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Objections

5. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claim 20 been renumbered 18.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1, 2, and 5-18 are rejected under 35 U.S.C. 102(e) as being anticipated by John B. Beavers (US 2003/0221123 A1, hereafter Beavers).

Regarding claim 1, Beavers teaches a network security system, comprising:

a static policy data store [*set of rules*, claim 1 and *rule engine,* Figure 5 (27)] having a static policy data attribute [*customer-specific enterprise rules*, Paragraph 0075];

a dynamic policy data store [*decision table*, claim 1 and Figure 5 (31); *dynamic threat table*, Paragraph 0054; *dynamic tracking table*, Paragraph 0098] for tracking a threat level associated with a connection [via *firewall* of Paragraphs 0002-0003 and

connection-monitoring *device experts* of Paragraphs 0104-0114, as well as *user tracking*, Paragraph 0094];

an authorization enforcement facility (AEF) [*alert processing system,* claim 12, figure 5 (63)] in communication with the static policy data store [*Rule Engine*, Figure 5 (27)] and the dynamic policy data store [*Decision Tables*, Figure 5 (31)] and operable to:

perform a risk-aware analysis [*matching* and *declaring an incident*, claim 1] of the connection to determine the threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection based at least in part on the static policy data attribute [*static enterprise data… such as lists of IP addresses that are associated with known attackers,* Paragraph 0077], and

store the determined threat level in the dynamic policy store as a dynamic policy data attribute [*assets… and… alerts/categories… automatically recorded… for later pattern recognition and possible automated declaration of incidents*, Paragraph 0054].

Regarding claim 2, Beavers teaches that the static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value [*a threshold value from a user-editable table*, claim 5], a node value, a service value, and an action value.

Regarding claim 5, Beavers teaches that the dynamic policy data store comprises a threat level table [*table with threat characterizations*, claim 5].

Regarding claim 6, Beavers teaches that the system is further operable to generate a response to the connection [*an action as a mitigating response can be taken*, Paragraph 0039].

Regarding claim 7, Beavers teaches that the response comprises at least one of blocking the source of the connection from connecting to an intended destination [*an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised,* Paragraph 0039], altering the intended destination of the connection [after an alert, *the information is trashed or diverted at line 25*, Paragraph 0033], or auditing the connection [Paragraph 0003].

Regarding claim 8, Beavers teaches that the AEF is further operable to generate a countermeasure [*an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised*, Paragraph 0039].

Regarding claim 9, Beavers teaches that the countermeasure comprises a passive countermeasure [Beavers: *an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised*, Paragraph 0039].

Regarding claim 10, Beavers teaches that the system comprises a router, a gateway, a hardware appliance [*firewall, IDS, router,* etc., Paragraphs 0105-0114], or a web server [claim 15].

Regarding claim 11, Beavers teaches that the system further comprises a firewall [Paragraph 0109] in communication with the AEF [*alert processing system*].

Regarding claim 12, Beavers teaches that the system further comprises an intrusion detection system [*IDS,* Paragraph 0113] in communication with the AEF [*alert processing system*].

Regarding claim 13, Beavers teaches a method comprising:

receiving a static policy data attribute [*customer-specific enterprise rules*, Paragraph 0075] from a static policy data store [*set of rules,* claim 1; Fig 5 (27)];

receiving a connection request directed to a node [Paragraphs 0002-0003];

determining a threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection [via *firewall* of Paragraphs 0002-0003 and connection-monitoring *device experts* of Paragraphs 0104-0114] based at least in part on the static policy data attribute [*set of rules,* claim 1 including *customer-specific enterprise rules*, Paragraph 0075] ; and

storing the threat level associated with the connection request as a dynamic policy data attribute [*assets… and… alerts/categories… automatically recorded… for*

later pattern recognition and possible automated declaration of incidents, Paragraph 0054] in a dynamic policy data store [*decision table,* claim 1].

Regarding claim 14, the claim comprises the limitations of claims 13 and 6 and is rejected by the same rationale.

Regarding claim 15, the claim comprises the limitations of claims 14 and 7 and is rejected by the same rationale.

Regarding claim 16, Beavers teaches updating the dynamic policy data attribute in the dynamic policy data store based on a result of the determining [*incident tracking rules can be automatically updated based on one or more further alert indications*, Paragraph 0015].

Regarding claim 17, Beavers teaches increasing a threat level if the connection request is determined to be anomalous [*If the non-condition alert passes the threshold, this information can be added to existing incident tickets, and the incident ticket tracking rules can be updated with this information*, Paragraph 0097; the rules referencing *the table with the time, the status, the threat level, and an incident description*, Paragraph 0040].

Regarding claim 18, Beavers teaches a network security system, comprising:

a static policy data store [*set of rules*, claim 1 and *rule engine*, Figure 5 (27)] having a static policy data attribute [*customer-specific enterprise rules*, Paragraph 0075];

a dynamic policy data store [*decision table*, claim 1 and Figure 5 (31); *dynamic threat table*, Paragraph 0054; *dynamic tracking table*, Paragraph 0098] for tracking a threat level associated with a connection [via *firewall* of Paragraphs 0002-0003 and connection-monitoring *device experts* of Paragraphs 0104-0114, as well as *user tracking*, Paragraph 0094];

an authorization enforcement facility (AEF) [*alert processing system,* claim 12, figure 5 (63)] in communication with the static policy data store [*Rule Engine*, Figure 5 (27)] and the dynamic policy data store [*Decision Tables*, Figure 5 (31)] and operable to:

perform a risk-aware analysis [*matching* and *declaring an incident*, claim 1] of the connection to determine the threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection based at least in part on the static policy data attribute [*static enterprise data… such as lists of IP addresses that are associated with known attackers,* Paragraph 0077],

store the determined threat level in the dynamic policy store as a dynamic policy data attribute [*assets… and… alerts/categories… automatically recorded… for later pattern recognition and possible automated declaration of incidents*, Paragraph 0054], and

generate a countermeasure, the countermeasure comprising an active countermeasure or a passive countermeasure [*an action as a mitigating response can*

be taken. An example would be to shut down a web server that is suspected of being compromised, Paragraph 0039].

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beavers in further view of Frederick M. Avolio (*Best Practices in Network Security*, hereafter *Avolio*).

Regarding claim 3, Beavers states that "the threshold value can be a level of severity" [Paragraph 0013] and that severity is defined "on a scale of 1-5 (1 being the highest threat)" [Paragraph 0036]. Beavers does not explicitly disclose that *the threshold value is inversely proportional to the node value*.

However, Avolio teaches [Avolio: Page 2 Column 3] that the severity of a threat is based upon the value of the object (e.g., a node) being secured (i.e., such that the higher the value of an object, the lower the threshold value is set or *setting the threshold value inversely proportional to the node value*).

Beavers and Avolio are analogous subject matter in the same field of endeavor as both cover network security systems. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the threshold-severity relation taught by Beavers with the severity-value relation taught by Avolio because

doing so allows for a basis by which to set the severity, and hence the threshold, level for object [Avolio: Page 2 Column 3].

Regarding claim 4, Beavers-Avolio teaches that *the threshold value is inversely proportional to the service value* [Avolio: Page 2 Columns 2-3, as the "object" can be a service].

10. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Iven Connary et al. (US 2004/0044912, hereinafter *Connary*) in view of Mark Cunningham et al. (US 6219786 B1, hereinafter *Cunningham*).

Regarding claims 1 and 13, Connary teaches *a network security system* and associated method, *comprising:*

a static policy data store [Connary: Paragraph 0016, "rules from a memory"] *having a static policy data attribute* [Paragraph 0014, "rules... set by a network administrator"];

a dynamic policy data store [Connary: Paragraph 0012 "store the determined threat level data in its memory"] *for tracking a threat level associated with a* source, event and destination [Connary: Paragraphs 0010 and 0004];

an authorization enforcement facility (AEF) [Connary: Paragraph 0014, "management module, event storage module"] *in communication with the static policy data store and the dynamic policy data store and operable to:*

perform a risk-aware analysis [Connary: Paragraph 0106] *of the connection to determine the threat level associated with the connection based at least in part on the static policy data attribute* [Connary: Paragraph 0014, "apply rules to threat level data"] *and*

store the determined threat level in the dynamic policy store as a dynamic policy data attribute [Connary: Paragraph 0010, "store the determined threat level data in its memory", "supply the alert data… [for writing] onto a storage medium" and Figure 26].

Connary does not explicitly disclose that the threat level is associated with *a connection*.

However, Cunningham discloses that the threat level is associated with *a connection* [Cunningham: Figure 7 Step 92].

Connary and Cunningham are analogous art in the same field of endeavor as both describe network security systems. It would have been obvious for one of ordinary skill in the art at the time the invention was made to utilize the connection-oriented scheme of Cunningham for identifying particular connections in the security system of Connary. One of ordinary skill in the art would have been motivated to modify the security system of Connary with the connection-oriented scheme of Cunningham because in doing so, the system would allow for targeting countermeasures at particular connections instead of all users.

Regarding claim 2, Connary-Cunningham teaches that *the static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value, a node value, a service value, or an action value* [Connary: Paragraph 0084].

Regarding claim 3, Connary-Cunningham teaches that *the threshold value is inversely proportional to the node value* [Connary: Paragraph 0111 and 0084 (the threshold is kept the same while the threat level is multiplied proportional to the node/service "destination" value, which is functionally equivalent to the claimed limitation)].

Regarding claim 4, Connary-Cunningham teaches that *the threshold value is inversely proportional to the service value* [Connary: Paragraph 0111 and 0084 (the threshold is kept the same while the threat level is multiplied proportional to the node/service "destination" value, which is functionally equivalent to the claimed limitation)].

Regarding claim 5, Connary-Cunningham teaches that *the dynamic policy data store comprises a threat level table* [Connary: Figure 26].

Regarding claims 6 and 14, Connary-Cunningham teaches that *the AEF is further operable to generate a response to the connection* [Cunningham: Column 11 Lines 3-13].

Regarding claim 7 and 15, Connary-Cunningham teaches that *the response comprises at least one of blocking the source of the connection from connecting to an intended destination, altering the intended destination of the connection, or auditing the connection* [Cunningham: Column 11 Lines 3-13].

Regarding claim 8, Connary-Cunningham teaches that *the AEF is further operable to generate a countermeasure* [Cunningham: Column 11 Lines 3-13].

Regarding claim 9, Connary-Cunningham teaches that *the countermeasure comprises an active countermeasure or a passive countermeasure* [Cunningham: Column 11 Lines 3-13].

Regarding claim 10, Connary-Cunningham teaches that *the AEF comprises a router, a gateway, a hardware appliance, or a web server* [Connary: Paragraph 0082 and Figure 1].

Regarding claim 11, Connary-Cunningham teaches *a firewall in communication with the AEF* [Connary: Paragraph 0082 and Figure 1].

Regarding claim 12, Connary-Cunningham teaches *an intrusion detection system in communication with the AEF* [Connary: Paragraph 0082 and Figure 1].

Regarding claim 16, Connary-Cunningham teaches *updating the dynamic policy data attribute in the dynamic policy data store based on a result of the determination* [Connary: Paragraph 0010].

Regarding claim 17, Connary-Cunningham teaches that *the updating comprises increasing the threat level if the connection request is determined to be anomalous* [Connary: Paragraph 0010].

Regarding claim 18, Connary teaches *a network security system* and associated method, *comprising:*

a static policy data store [Connary: Paragraph 0016, "rules from a memory"] *having a static policy data attribute* [Paragraph 0014, "rules... set by a network administrator"];

a dynamic policy data store [Connary: Paragraph 0012 "store the determined threat level data in its memory"] *for tracking a threat level associated with a* source, event and destination [Connary: Paragraphs 0010 and 0004];

an authorization enforcement facility (AEF) [Connary: Paragraph 0014, "management module, event storage module"] *in communication with the static policy data store and the dynamic policy data store and operable to:*

perform a risk-aware analysis [Connary: Paragraph 0106] *of the connection to determine the threat level associated with the connection based at least in part on the static policy data attribute* [Connary: Paragraph 0014, "apply rules to threat level data"]

and

store the determined threat level in the dynamic policy store as a dynamic policy data attribute [Connary: Paragraph 0010, "store the determined threat level data in its memory", "supply the alert data… [for writing] onto a storage medium" and Figure 26].

Connary does not explicitly disclose that the threat level is associated with *a connection* or that the AEF is operable to *generate a countermeasure, the countermeasure comprising an active countermeasure or a passive countermeasure.*

However, Cunningham discloses that the threat level is associated with *a connection* [Cunningham: Figure 7 Step 92] and that the AEF is operable to *generate a countermeasure, the countermeasure comprising an active countermeasure or a passive countermeasure* [Cunningham: Column 11 Lines 3-13].

Connary and Cunningham are analogous art in the same field of endeavor as both describe network security systems. It would have been obvious for one of ordinary skill in the art at the time the invention was made to utilize the connection-oriented scheme of Cunningham for identifying particular connections in the security system of Connary. One of ordinary skill in the art would have been motivated to modify the security system of Connary with the connection-oriented scheme of Cunningham because in doing so, the system would allow for targeting countermeasures at particular connections instead of all users.

Conclusion

11. **Examiner's Note:** Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IMAD HUSSAIN whose telephone number is (571) 270-3628. The examiner can normally be reached on Monday through Friday from 0730 to 1630.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/IH/
Imad Hussain
Examiner, Art Unit 2151
/Salad Abdullahi/
Primary Examiner, Art Unit 2157